### matchfeed()

Returns true if the threat intelligence feed contains a target value, and false otherwise.

#### Syntax

matchfeed(FEED\_ID, STR\_EXPR)

Required Parameter

**FEED\_ID**

Identifier of the threat intelligence feed. If you specify an invalid feed string constant, the query fails.

See the following table for available identifiers. In addition, you can use the feeds provided by apps installed on Logpresso Sonar or Logpresso Maestro.

|  |  |  |
| --- | --- | --- |
| FEED\_ID | Type | Description |
| otx | ip | Real-time IP address reputation feed in the format of OTX (Open Threat Exchange) |
| tor | ip | Real-time Tor exit node IP address information feed |
| mdl\_domain | domain | Real-time malicious domain name (e.g. C&C domain) |
| mdl\_ip | ip | Real-time malicious domain name (e.g. C&C IP address) |
| abusech | domain | Real-time malicious domain name (e.g. C&C domain) feed provided by abuse.ch |
| malc0de | md5 | Real-time Malware database provided by malc0de.com |

**STR\_EXPR**

Expression to return the string to be searched in the feed